AF #

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT	:	Mohamed Abdel-Mottaleb		
SERIAL NO.	:	09/419,671	EXAMINER	: Cas P. Stulberger
FILED	:	October 15, 1999	ART UNIT	: 2132
FOR	:	IMAGE AND VIDEO AUTHENTICATION SYSTEM		

APPEAL BRIEF TRANSMITTAL LETTER

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA. 22313-1450

Dear Sir:

Appellants respectfully submit three copies of an Appeal Brief For Appellants that includes an Appendix with the pending claims. The Appeal Brief is now due on April 8, 2005.

Appellants enclose a check in the amount of $500.00 covering the requisite Government Fee.

Should the Examiner deem that there are any issues which may be best resolved by telephone communication, kindly telephone Applicants undersigned representative at the number listed below.

Respectfully submitted,
Russell Gross
Registration No. 40,007

By: Steve Cha
Attorney for Applicant
Registration No. 44,069

Date: 4/1/05

Mail all correspondence to:
Russell Gross, Registration No. 40,007
US PHILIPS CORPORATION
P.O. Box 3001
Briarcliff Manor, NY 10510-8001
Phone: (914) 333-9608
Fax: (914) 332-0615

Certificate of Mailing Under 37 CFR 1.8

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to MAIL STOP APPEAL BRIEF-PATENTS, COMMISSIONER FOR PATENTS, P.O. BOX 1450, ALEXANDRIA, VA. 22313 on 4/1/05.

Steve Cha, Reg. No. 44,069
(Name of Registered Rep.)

4/1/05
(Signature and Date)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Before the Board of Patent Appeals and Interferences

In re the Application

Inventor	:	**Mohamed Abdel-Mottaleb**
Application No.	:	**09/419,671**
Filed	:	**October 15, 1999**
For	:	**IMAGE AND VIDEO AUTHENTICATION SYSTEM**

APPEAL BRIEF

On Appeal from Group Art Unit 2132

Date: April 1, 2005

By: Russell Gross
Registration No. 40,007
Steve Cha
Attorney for Applicant
Registration No. 44,069

Certificate of Mailing Under 37 CFR 1.8

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to MAIL STOP APPEAL BRIEF-PATENTS, COMMISSIONER FOR PATENTS, P.O. BOX 1450, ALEXANDRIA, VA. 22313 on April 1, 2005.

Steve Cha, Reg. No. 44,069
(Name of Registered Rep.)

(Signature and Date)

04/05/2005 MAHMED1 00000013 09419671
01 FC:1402 500.00 OP

		Page
I.	REAL PARTY IN INTEREST.....	3
II.	RELATED APPEALS AND INTERFERENCES.....	3
III.	STATUS OF CLAIMS.....	3
IV.	STATUS OF AMENDMENTS.....	3
V.	SUMMARY OF THE CLAIMED SUBJECT MATTER...	4
VI.	GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL	5
VII.	ARGUMENT.....	5
VIII.	CONCLUSION.....	11
IX.	APPENDIX: THE CLAIMS ON APPEAL.....	12

I. REAL PARTY IN INTEREST

The real party in interest is the assignee of the present application, Philips Electronic North America Corporation, and not the party named in the above caption.

II. RELATED APPEALS AND INTERFERENCES

With regard to identifying by number and filing date all other appeals or interferences known to Appellant which will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal, Appellant is not aware of any such appeals or interferences.

III. STATUS OF CLAIMS

Claims 1-20 have been presented for examination. The statuses of claims 1-20 are, respectively: (1) previously presented, (2)-(6) original, (7)-(8) canceled, (9) previously presented, (10)-(16) original, (17)-(18) canceled, (19) previously presented, and (20) original. All of these claims are pending, stand finally rejected, and are being appealed.

IV. STATUS OF AMENDMENTS

No amendment after final rejection has been filed. A request for reconsideration after final was filed December 22, 2004.

V. SUMMARY of the CLAIMED SUBJECT MATTER

An image signal is authenticated by embodying unobtrusively, within the signal, a signature based uniquely on the content of the image (page 3, lines 4-6). Tampering with the image, e.g., so as to manipulate the signal, may occur by unauthorized intervention when the signal is in transit or by retrieval of the received and stored image (page 2, lines 3-6). The impairment can be detected by comparing the signature with the image content, and noticing a mismatch (page 2, lines 19-21).

The authenticating involves generating a transform representation of the image and determining a digital signature unique to the image (page 3, lines 4-7). High frequency coefficients within the transform representation are identified (page 7, lines 5-6). The coefficients are assigned values to correspond to the digital signature, which has a plurality of digits (page 5, lines 14-15; page 7, lines 6-7). The transform representation of the image includes a plurality of blocks that each have at least one high frequency coefficient (page 8, lines 19-21). The assigning of coefficient values involves assigning, to one coefficient in each block, a value that corresponds to one of the digits of the signature (page 7, line 22 – page 8, line 10).

Advantageously, the present invention conserves signature bits or "digits." In particular, in a preferred embodiment, i) there are a greater number of blocks in the image representation than there are digits in the signature (page 9, lines 3-4); and ii) the assigning of coefficient values is accomplished by repeating the coefficient values corresponding to the signature a number of times such that each block includes a coefficient having a value corresponding to a signature digit (page 9, lines 2-7).

In a preferred embodiment, utilization is made of a preselected pattern of coefficient values that is representative of corresponding values in the digital signature.

Preferably, the digital signature is a binary number having a plurality of digits. Each digit has a value that is either 1 or 0. The preselected pattern includes assigning a first number value to a coefficient that corresponds to a signature digit having a value of 1 and assigning a second number value to a coefficient that corresponds to a signature digit having a value of 0. The first number value is an even number value and the second

number value is an odd number value (page 7, line 22 – page 8, line 10; page 10, lines 22-23).

VI. GROUND of REJECTION to be REVIEWED ON APPEAL

The ground of rejection submitted for review on appeal is whether claims 1-6, 9-16, 19 and 20 are invalidly rejected under 35 U.S.C. 102(e) as anticipated by U.S. Patent No. 6,064,764 to Bhaskaran.

VII. ARGUMENT

Rejection of claims 1-3, 5, 9-13, 16, 19 and 20 under 35 U.S.C. 102(e) over Bhaskaran

Claim 1 recites:

> A method . . . comprising the steps of: . . . (B) determining a digital signature . . .; and (D) assigning . . . to the digital signature, wherein . . . the transform representation of the image includes a plurality of blocks that each have at least one high frequency coefficient . . . and step (D) further includes repeating the coefficient values corresponding to the signature . . . such that each block includes a coefficient having a value corresponding to a signature digit

Bhaskaran, by contrast, although disclosing "a plurality of blocks that each have at least one high frequency coefficient," i) skips over blocks whose 63rd coefficient is low-valued; and ii) halts when the signature is embedded.

As a consequence and correspondingly, Bhaskaran fails to disclose or suggest a) "repeating . . . such that each block includes a coefficient having a value corresponding to a signature digit"; and b) "repeating the coefficient values corresponding to the signature

. . . such that each block includes a coefficient having a value corresponding to a signature digit."

In the discussion that follows, item b) is addressed first. Then, item a) is discussed.

Item b)

As to item b), the last two sentences of the Advisory Action, continuation of item 5, incorrectly suggest that Bhaskaran features the "repeating" of claim 1 by virtue of the Bhaskaran second pass. In particular, the Advisory Action seems to suggest that the Bhaskaran first pass embeds the bits of Bhaskaran watermark W and that the second pass repeats the embedding of those bits of the Bhaskaran watermark W.

This suggestion by the Advisory Action is incorrect, at least because, although the Bhaskaran second pass embeds bits of the watermark W, the Bhaskaran first pass does not.

In particular, the Bhaskaran embedding of watermark W bits occurs in the second pass, occurs once, and is not repeated for those bits.

As a preliminary matter, the applicant notes that Bhaskaran is directed to watermarking an image (col. 4, line 10), e.g., a JPEG image I (col. 4, line 21). The image is composed of macroblocks, each of which has 16 rows, and 16 columns, of pixels. Each macroblock has four quadrants, each of which has 8 x 8 pixels (col. 4, line 25: line 25: "8 x 8"). Bhaskaran refers to a quadrant as a block (col. 4, lines 22-29).

To watermark the image I, Bhaskaran makes two passes (col. 4, lines 11-17). Bhaskaran performs the embedding of watermark W bits only in the second pass of the two-pass procedure (col. 4, lines 10(11)-16(17)).

With respect to the Bhaskaran m-bit watermark W, at the outset of the Bhaskaran two-pass procedure, the value of "m" is unknown; however, a minimum value for "m" may be pre-specified. The m-bit Bhaskaran watermark W, which is generated at the end of the first pass (FIG. 2, step 109), will be comprised of number of bits that is greater or equal to that pre-specified bit-length (col. 5, lines 29-33).

The Bhaskaran first pass selectively determines which blocks are to receive a bit of watermark W (FIG. 2, step 106). The Bhaskaran second pass embeds each of the m bits of watermark W in the respective one of the blocks that was chosen in the first pass (FIG. 3, steps 206, 207; col. 4, line 63 – col. 5, line 3; col. 5, line 66 – col. 6, line 7). Once the m bits are embedded, during the second pass, in the blocks selectively chosen in the first pass, no more blocks pre-chosen in the first pass exist, and the two-pass procedure then halts (FIG. 3, step 203, "NO" branch).

Notably the m bits are generated at the conclusion of the first pass for image I (col. 5, lines 43-46). The generated m bits of watermark W are uniquely representative of the image I being watermarked (FIG. 2, step 108). The generated m bits are embedded, during the second pass, in the m blocks of image I chosen in the first pass (FIG. 2, steps 106, 107; FIG. 3, steps 206, 207; col. 4, lines 10(11)-16(17)).

In effect, the first pass tailors the value "m" to the number of blocks in image I that are found to be suitable for embedding a bit (FIG. 2, step 106), subject to "m" being greater or equal to any minimum bit-length pre-specified (col. 5, lines 29-33; col. 3, lines 4-5). Those m bits of the watermark to be embedded are generated at the conclusion of the first pass (col. 5, lines 43-46), and embedded during the second pass (FIG. 3, steps

206, 207). Bhaskaran fails to disclose or suggest any repetition of the embedding of those m bits. Nor can the present applicant think of any reason to do so.

In particular Bhaskaran fails to disclose or suggest:

> A method . . . comprising the steps of: . . . (B) determining a digital signature . . .; and (D) assigning . . . to the digital signature, wherein . . . the transform representation of the image includes a plurality of blocks that each have at least one high frequency coefficient . . . and step (D) further includes repeating the coefficient values corresponding to the signature . . . such that each block includes a coefficient having a value corresponding to a signature digit

For at least the foregoing reasons pertaining to item b) above, Bhaskaran fails to anticipate the present invention as recited in claim 1.

Item a)

Item a) is reiterated immediately below.

Bhaskaran fails to disclose or suggest a) "repeating . . . such that each block includes a coefficient having a value corresponding to a signature digit"

The Advisory Action states:

> A hash function is applied at each block and after a watermark is computed each watermark bit is embedded in one of the blocks it was previously determined to do so (Bhaskaran: column 3, lines 1-17)

This statement by the Advisory Action refers to lines 14 and 15 of column 3 in Bhaskaran, which recite, ". . . each watermark bit is embedded in one of the blocks for which it was previously determined to do so . . ."

As set forth above in the instant appeal brief, each of the m bits of the Bhaskaran watermark W is, during the second pass, embedded in one of the blocks of the image I (FIG. 3, steps 206, 207). In particular, this one block is the block chosen, during the first pass, for the respective bit (col. 4, line 63 – col. 5, line 3; col. 5, line 66 – col. 6, line 7).

Specifically, every time a block is chosen in the first pass, a bit of the watermark W is assigned to that block. If, during the first pass, a next block is then found suitable, another bit is assigned to that next block (FIG. 2, steps 106, 107).

Notably, and referring again to lines 14 and 15 of column 3 in Bhaskaran, they recite, ". . . each watermark bit is embedded in one of the blocks for which it was previously determined to do so . . ."

In particular, Bhaskaran, in choosing blocks during the first pass, skips over certain blocks.

To save bandwidth and/or storage, "only those blocks are chosen to embed a watermark bit where the 63rd coefficient is already non-zero," and "we do not choose as embedders even the blocks where the 63rd coefficient (dequantized) is plus or minus 1" (col. 5, lines 17-19, 24-26).

Since Bhaskaran skips over certain blocks, Bhaskaran fails to disclose or suggest a) "repeating . . . such that each block includes a coefficient having a value corresponding to a signature digit" which language explicitly appears in the present claim 1.

For this reason too, Bhaskaran fails to anticipate the present invention as recited in claim 1.

Notably, and in addition, there is no suggestion in Bhaskaran of giving up the bandwidth/storage advantage to embed into every block. Such modification of Bhaskaran would amount to impermissible hindsight by an Examiner who has seen the disclosure of the present invention.

The hypothetical goal of embedding into more blocks, or, better yet, into every block to more resemble the present claim 1, for the sake of increasing robustness, amounts to impermissible hindsight.

Moreover, even if Bhaskaran were modified to forego skipping any blocks, the Bhaskaran first pass would still generate a single watermark W, and the Bhaskaran second pass would still embed W bit-by-bit and then halt. Accordingly, such a modified Bhaskaran embodiment would still not feature item b), i.e., "repeating the coefficient values corresponding to the signature . . . such that each block includes a coefficient having a value corresponding to a signature digit."

For at least all of the above reasons, Bhaskaran fails to disclose or suggest, a) "repeating . . . such that each block includes a coefficient having a value corresponding to a signature digit"; and b) "repeating the coefficient values corresponding to the signature . . . such that each block includes a coefficient having a value corresponding to a signature digit."

For at least the foregoing reasons, claim 1 is not rendered obvious by Bhaskaran, and the applicant does not believe that any modification of Bhaskaran to resemble claim 1 would have been obvious.

Claims 9 and 19 are system and software claims corresponding to method claim 1, and are likewise deemed to distinguish patentably over the applied reference.

Rejection of claims 4, 6, 14 and 15 under 35 U.S.C. 102(e) over Bhaskaran

Claims 4, 6, 14 and 15 depend from base claims 1 and 9, and are therefore deemed to distinguish patentably over Bhaskaran for at least the same respective reasons set forth above with regard to claims 1 and 9.

In addition, claims 4, 6, 14 and 15 are separately patentable, since each of these claims recites an "even number value" for a "first number value" assigned "to a coefficient that corresponds to a signature digit having a value of 1."

Bhaskaran, by contrast, sets the coefficient to equal the bit of watermark W, i.e., what the Office Action and Advisory Action regard as corresponding to the "signature digit" of the present invention (Bhaskaran, FIG. 3, step 207: "equal"). Accordingly, in the case of the Bhaskaran bit being 1, the number 1 is not an "even number" which term explicitly appears in claims 4, 6, 14 and 15 of the present invention. For this reason too, therefore, Bhaskaran fails to anticipate the present invention as recited in claims 4, 6, 14 and 15.

VIII. CONCLUSION

In view of the above analysis, it is respectfully submitted that the referenced teachings, whether taken individually or in combination, fail to anticipate or render obvious the subject matter of any of the present claims. Therefore, reversal of all outstanding grounds of rejection is respectfully solicited.

Respectfully submitted,

Date: 4/1/05

By: Steve Cha
Attorney for Applicant
Registration No. 44,069

IX. APPENDIX: THE CLAIMS ON APPEAL

1. (previously presented) A method of authenticating an image signal, comprising the steps of

(A) generating a transform representation of the image;

(B) determining a digital signature unique to the image;

(C) identifying high frequency coefficients within the transform representation; and

(D) assigning values to the high frequency coefficients to correspond to the digital signature, wherein the digital signature has a plurality of digits, the transform representation of the image includes a plurality of blocks that each have at least one high frequency coefficient and step (D) includes assigning a value to one coefficient in each block that corresponds to one of the digits of the signature; and

wherein there are a greater number of blocks in the image representation than there are digits in the signature and step (D) further includes repeating the coefficient values corresponding to the signature a number of times such that each block includes a coefficient having a value corresponding to a signature digit.

2. (original) The method of claim 1, wherein step (D) includes using a preselected pattern of coefficient values that is representative of corresponding values in the digital signature.

3. (original) The method of claim 2, wherein the digital signature is a binary number having a plurality of digits, wherein each digit has a value that is either 1 or 0 and wherein the preselected pattern includes assigning a first number value to a coefficient that corresponds to a signature digit having a value of 1 and assigning a second number value to a coefficient that corresponds to a signature digit having a value of 0.

4. (original) The method of claim 3, wherein the first number value is an even number value and the second number value is an odd number value.

4. (original) The method of claim 2, wherein the digital signature is a binary number having a plurality of digits, wherein each digit has a value that is either 1 or 0 and wherein the preselected pattern includes assigning a first chosen number value to multiple coefficients that collectively correspond to a signature digit having a value of 1 and assigning a second chosen number value to multiple coefficients that collectively correspond to a signature digit having a value of 0.

6. (original) The method of claim 5, wherein the first chosen number value is an even number value and the second chosen number value is an odd number value.

7. (canceled)

8. (canceled)

9. (previously presented) A system for authenticating an image signal, comprising:

a transform module that generates a transform representation of the image that includes high frequency coefficients;

a signature extractor module that generates a digital signature unique to the image; and

a signature embedding module that assigns values to the high frequency coefficients that correspond to the digital signature, wherein the digital signature has a plurality of digits, the transform representation of the image includes a plurality of blocks that each have at least one high frequency coefficient and the signature embedding module assigns a value to one coefficient in each block that corresponds to one of the digits of the signature; and

wherein there are a greater number of blocks in the image representation than there are digits in the signature and the signature embedding module repeats the coefficient values corresponding to the signature a number of times such that each block includes a coefficient having a value corresponding to a signature digit.

10. (original) The system of claim 9, wherein each of the modules is embodied in a computer.

11. (original) The system of claim 10, wherein each of the modules comprises software.

12. (original) The system of claim 9, wherein the signature embedding module uses a preselected pattern of coefficient values that is representative of corresponding values in the digital signature.

13. (original) The system of claim 12, wherein the digital signature is a binary number having a plurality of digits, wherein each digit has a value that is either 1 or 0 and wherein the preselected pattern includes a first number value for each coefficient that corresponds to a signature digit having a value of 1 and a second number value for each coefficient that corresponds to a signature digit having a value of 0.

14. (original) The system of claim 13, wherein the first number value is an even number value and the second number value is an odd number value.

15. (original) The system of claim 12, wherein the digital signal is a binary number having a plurality of digits, wherein each digit has a value that is either 1 or 0 and wherein the preselected pattern includes a first chosen number value assigned to multiple coefficients that collectively correspond to a signature digit having a value of 1 and a second chosen number value assigned to multiple coefficients that collectively correspond to a signature digit having a value of 0.

16. (original) The system of claim 15, wherein the first chosen number value is an even number value and the second chosen number value is an odd number value.

17. (canceled)

18. (canceled)

19. (previously presented) A computer readable medium having a plurality of computer-executable instructions for authenticating an image signal, comprising:

a first program module that directs the computer to generate a transform representation of the image that includes high frequency coefficients;

a second program module that directs the computer to determine a digital signature unique to the image; and

a third program module that directs the computer to assign values to the high frequency coefficients to correspond to the digital signature, wherein the digital signature has a plurality of digits, the transform representation of the image includes a plurality of blocks that each have at least one high frequency coefficient and the assigning includes assigning a value to one coefficient in each block that corresponds to one of the digits of the signature; and

wherein there are a greater number of blocks in the image representation than there are digits in the signature and the assigning by the computer further includes repeating the coefficient values corresponding to the signature a number of times such that each block includes a coefficient having a value corresponding to a signature digit.

20. (original) The computer-readable medium of claim 19, wherein the third program module assigns values to the high frequency coefficients according to a preselected pattern such that the values assigned to the high frequency coefficients are decipherable to indicate the image signature.